

Japanese Patent Laid-open Publication No. 2003-22009 A

Publication date: January 24, 2003

Applicant: : NEC CORP

Title: Simplified data authenticity guarantee system, method, and program

5

(57) [Abstract]

[Object] In a general transaction processing system, it is an object to realize guarantee of data authenticity, with a cheap configuration and without requiring special hardware.

10 [Means] A data authenticity guarantee server comprises: a unit that backs up a file in a transaction processing system to a mass storage at a predetermined timing; a unit that generates a hash value by a hash function, using the file as a parameter, along with the backup, and stores it in a memory; a unit that reads the file from the transaction processing system based on a request for verifying the authenticity,
15 generates a hash value by the hash function, using the file as a parameter, reads the hash value at the time of the previous hash from the memory, and compares it with a newly generated hash value, to verify the data authenticity; and a unit that determines that the data has been falsified, when these do not agree with each other as a result of comparison of hash values, and restores the file based on the backup file stored in the
20 mass storage.

[What is Claimed is]

[Claim 1] A simplified data authenticity guarantee system having a transaction processing system, a mass storage, and a data authenticity guarantee server, wherein

25 the data authenticity guarantee server comprises:

a unit that backs up a file in the transaction processing system, for which the authenticity is to be secured, to a mass storage at a predetermined timing;

a unit that generates a hash value by a hash function, using the file as a parameter, along with the backup by the unit, and stores the hash value in a memory;

5 a unit that reads the file from the transaction processing system based on a request for verifying the authenticity of the file, generates a hash value by the hash function by using the file as a parameter, reads the hash value of the file at the time of the previous hash from the memory, and compares it with a newly generated hash value, to verify the data authenticity; and

10 a unit that determines that the data has been falsified, when these do not agree with each other as a result of comparison of hash values, and restores the file based on the backup file stored in the mass storage.

[Claim 2] The simplified data authenticity guarantee system according to claim 1, further comprising:

15 a unit that adds an electronic signature to the hash value, at the time of hash along with the backup; and

a unit that verifies the authenticity of the electronic signature added to the previous hash value, at the time of verifying the data authenticity.

[Claim 3] The simplified data authenticity guarantee system according to claim 20 1 or 2, further comprising a unit that records the process of authenticity verification of the file in a log file.

[Claim 4] The simplified data authenticity guarantee system according to any one of claims 1 to 3, further comprising a unit that notifies an administrator of the result of authenticity verification relating to the file.

25 [Claim 5] A simplified data authenticity guarantee method for securing the data

authenticity of a file held by a transaction processing system, wherein

a data authenticity guarantee server comprises:

a step of backing up the file in the transaction processing system, for which the authenticity is to be secured, to a mass storage at a predetermined timing;

5 a step of generating a hash value by a hash function, using the file as a parameter, along with the backup, and storing the hash value in a memory;

a step of reading the file from the transaction processing system based on a request for verifying the authenticity of the file, generating a hash value by the hash function by using the file as a parameter, reading the hash value of the file at the time of
10 the previous hash from the memory, and comparing it with a newly generated hash value, to verify the data authenticity; and

a step of determining that the data has been falsified, when these do not agree with each other as a result of comparison of the hash values, and restoring the file based on the backup file stored in the mass storage.

15 [Claim 6] The simplified data authenticity guarantee method according to claim 5, further comprising:

a step of adding an electronic signature to the hash value, at the time of hash along with the backup; and

a step of verifying the authenticity of the electronic signature added to the
20 previous hash value, at the time of verifying the data authenticity.

[Claim 7] The simplified data authenticity guarantee method according to claim 5 or 6, further comprising a step of recording the process of authenticity verification of the file in a log file.

[Claim 8] The simplified data authenticity guarantee method according to any
25 one of claims 5 to 7, further comprising a step of notifying an administrator of the result

of authenticity verification relating to the file.

[Claim 9] A simplified data authenticity guarantee program for securing the data authenticity of a file held by a transaction processing system, which makes a data authenticity guarantee server execute:

- 5 a process for backing up the file in the transaction processing system, for which the authenticity is to be secured, to a mass storage at a predetermined timing;
- a process for generating a hash value by a hash function, using the file as a parameter, along with the backup, and storing the hash value in a memory;
- a process for reading the file from the transaction processing system based
- 10 on a request for verifying the authenticity of the file, generating a hash value by the hash function by using the file as a parameter, reading the hash value of the file at the time of the previous hash from the memory, and comparing it with a newly generated hash value, to verify the data authenticity; and
- a process for determining that the data has been falsified, when these do not
- 15 agree with each other as a result of comparison of the hash values, and restoring the file based on the backup file stored in the mass storage.

Fig. 1 is a diagram of the configuration of a simplified data authenticity guarantee system in the first embodiment of the present invention.

20

[Explanation of Reference Signs]

- 100 General transaction processing system
- 200 Document storage
- 201 Large capacity backup file storage section
- 25 300 Data authenticity guarantee server

- 301 Data backup processor
- 302 Hash value generation processor
- 303 Data substantially verification processor
- 304 Data restoration processor

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-22009

(P2003-22009A)

(43)公開日 平成15年1月24日(2003.1.24)

(51)Int.Cl. ⁷	識別記号	F I	データ(参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D 5 J 1 0 4 6 4 0 A

審査請求 有 請求項の数12 O L (全 8 頁)

(21)出願番号 特願2001-209226(P2001-209226)

(22)出願日 平成13年7月10日(2001.7.10)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 有福 義範

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 峯尾 真一

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100084250

弁理士 丸山 隆夫

Fターム(参考) 5J104 AA08 LA05 NA12 PA07

(54)【発明の名称】 簡易型データ真正性保証システム、方法、およびプログラム

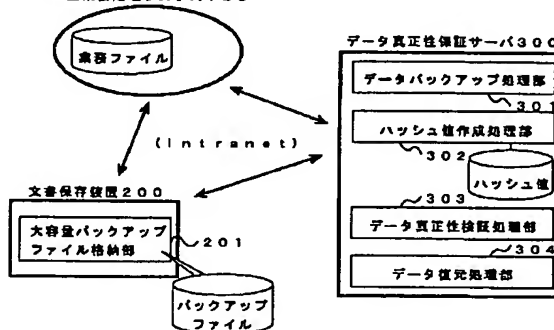
(57)【要約】

【課題】 一般業務処理システムなどにおいて、特別なハードウェア装置を必要とすることなく安価な構成で、データの真正性の保証を実現すること。

【解決手段】 データ真正性保証サーバは、所定のタイミングで、業務処理システム内のファイルを大容量記憶装置にバックアップする手段と、バックアップに伴い、前記ファイルを引数としてハッシュ関数によりハッシュ値を生成し、メモリに保存する手段と、真正性検証の要求に基づき、ファイルを業務処理システムから読み込み、ファイルを引数として前記ハッシュ関数によりハッシュ値を生成し、前回のハッシュ時のハッシュ値をメモリから読み出し、新たに生成したハッシュ値と比較してデータ真正性の検証を行う手段と、比較の結果、不一致の場合、データ改ざんが発生したと判断し、ファイルを前記大容量記憶装置に保存されているバックアップファイルをもとに復元する手段とを有する。

第1の実施例

一般業務処理システム100



【特許請求の範囲】

【請求項 1】 業務処理システムと、大容量記憶装置と、データ真正性保証サーバと、を有する簡易型データ真正性保証システムであって、前記データ真正性保証サーバは、所定のタイミングで、前記業務処理システム内の真正性保証対象のファイルを前記大容量記憶装置にバックアップする手段と、該手段によるバックアップに伴い、前記ファイルを引数としてハッシュ関数によりハッシュ値を生成し、該ハッシュ値をメモリに保存する手段と、前記ファイルについての真正性検証の要求に基づき、該ファイルを前記業務処理システムから読み込み、該ファイルを引数として前記ハッシュ関数によりハッシュ値を生成し、該ファイルについての前回のハッシュ時のハッシュ値を前記メモリから読み出し、前記新たに生成したハッシュ値と比較してデータ真正性の検証を行う手段と、前記ハッシュ値比較の結果、不一致の場合、前記ファイルについてデータ改ざんが発生したと判断し、該ファイルを前記大容量記憶装置に保存されているバックアップファイルをもとに復元する手段と、を有することを特徴とする簡易型データ真正性保証システム。

【請求項 2】 前記バックアップに伴うハッシュの際、前記ハッシュ値に電子署名を付加する手段と、前記データ真正性検証の際、前記前回のハッシュ値に付加されている電子署名の正当性を検証する手段と、をさらに有することを特徴とする請求項 1 記載の簡易型データ真正性保証システム。

【請求項 3】 前記ファイルについての真正性検証の過程を履歴ファイルに記録する手段をさらに有することを特徴とする請求項 1 または 2 に記載の簡易型データ真正性保証システム。

【請求項 4】 前記ファイルについての真正性検証の結果を管理者に通知する手段をさらに有することを特徴とする請求項 1 から 3 のいずれか 1 項に記載の簡易型データ真正性保証システム。

【請求項 5】 業務処理システムの保持するファイルについてデータの真正性を保証する簡易型データ真正性保証方法であって、データ真正性保証サーバが、所定のタイミングで、前記業務処理システム内の真正性保証対象であるファイルを大容量記憶装置にバックアップするステップと、該バックアップに伴い、前記ファイルを引数としてハッシュ関数によりハッシュ値を生成し、該ハッシュ値をメモリに保存するステップと、前記ファイルについての真正性検証の要求に基づき、該ファイルを前記業務処理システムから読み込み、該ファイルを引数として前記ハッシュ関数によりハッシュ値を

生成し、該ファイルについての前回のハッシュ時のハッシュ値を前記メモリから読み出し、前記新たに生成したハッシュ値と比較してデータ真正性の検証を行うステップと、前記ハッシュ値比較の結果、不一致の場合、前記ファイルについてデータ改ざんが発生したと判断し、該ファイルを前記大容量記憶装置に保存されているバックアップファイルをもとに復元するステップと、を有することを特徴とする簡易型データ真正性保証方法。

10 【請求項 6】 前記バックアップに伴うハッシュの際、前記ハッシュ値に電子署名を付加するステップと、前記データ真正性検証の際、前記前回のハッシュ値に付加されている電子署名の正当性を検証するステップと、をさらに有することを特徴とする請求項 5 記載の簡易型データ真正性保証方法。

【請求項 7】 前記ファイルについての真正性検証の過程を履歴ファイルに記録するステップをさらに有することを特徴とする請求項 5 または 6 に記載の簡易型データ真正性保証方法。

20 【請求項 8】 前記ファイルについての真正性検証の結果を管理者に通知するステップをさらに有することを特徴とする請求項 5 から 7 のいずれか 1 項に記載の簡易型データ真正性保証方法。

【請求項 9】 業務処理システムの保持するファイルについてデータの真正性を保証する簡易型データ真正性保証プログラムであって、データ真正性保証サーバに、所定のタイミングで、前記業務処理システム内の真正性保証対象であるファイルを大容量記憶装置にバックアップする処理と、

30 該バックアップに伴い、前記ファイルを引数としてハッシュ関数によりハッシュ値を生成し、該ハッシュ値をメモリに保存する処理と、

前記ファイルについての真正性検証の要求に基づき、該ファイルを前記業務処理システムから読み込み、該ファイルを引数として前記ハッシュ関数によりハッシュ値を生成し、該ファイルについての前回のハッシュ時のハッシュ値を前記メモリから読み出し、前記新たに生成したハッシュ値と比較してデータ真正性の検証を行う処理

40 と、前記ハッシュ値比較の結果、不一致の場合、前記ファイルについてデータ改ざんが発生したと判断し、該ファイルを前記大容量記憶装置に保存されているバックアップファイルをもとに復元する処理と、を実行させることを特徴とする簡易型データ真正性保証プログラム。

【請求項 10】 前記データ真正性保証サーバに、前記バックアップに伴うハッシュの際、前記ハッシュ値に電子署名を付加する処理と、前記データ真正性検証の際、前記前回のハッシュ値に付加されている電子署名の正当性を検証する処理と、をさ

らに実行させることを特徴とする請求項9記載の簡易型データ真正性保証プログラム。

【請求項11】 前記データ真正性保証サーバに、前記ファイルについての真正性検証の過程を履歴ファイルに記録する処理をさらに実行させることを特徴とする請求項9または10に記載の簡易型データ真正性保証プログラム。

【請求項12】 前記データ真正性保証サーバに、前記ファイルについての真正性検証の結果を管理者に通知する処理をさらに実行させることを特徴とする請求項9から11のいずれか1項に記載の簡易型データ真正性保証プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、イントラネット、業務処理システムなどにおけるデータ真正性保証システム、方法、およびプログラムに関する。

【0002】

【従来の技術】従来の業務処理システムは、外部からの社内ネットワーク（イントラネット）への不正侵入、あるいは、社内ネットワーク内部での不正侵入などによる、データの改ざん、破壊、契約の否認、成りすましなどの数多くの脅威に晒されており、これらを防止する十分な手段が無い状況にあった。

【0003】また、上記のような脅威を防止するための対策は、膨大な費用がかかるものであるため、社内ネットワークの内外部からの不正侵入に備えるシステムを構築する際の重要な課題が、費用対効果を策定することであった。

【0004】従来技術として、特開2000-228060号公報は、可搬型記憶媒体を用いたデータ記録／再生装置について開示している。この技術は、大容量の画像データなどを可搬型記録媒体に格納する際、データ内容の秘匿性・真正性を確保し、データの不正な消去、破壊を含めた改ざんを防止できるデータ記録／再生装置を提供するものである。

【0005】また、特開平10-326078号公報は、デジタル署名の方法について開示している。これは、特に、ネットワークを介して転送されるデータファイル、データストリームについてのより効率的なデジタル署名を提供することを意図した方法である。

【0006】

【発明が解決しようとする課題】本発明は、かかる問題点に鑑みてなされたものであり、一般の業務処理システムや計算センタや社内イントラネットなどにおいて、特別なハードウェア装置を必要とすることなく安価な構成でデータの真正性の保証を実現することのできる簡易型データ真正性保証システム、方法、およびプログラムを提供することを目的とする。

【0007】

【課題を解決するための手段】かかる目的を達成するために、請求項1記載の発明は、業務処理システムと、大容量記憶装置と、データ真正性保証サーバと、を有する簡易型データ真正性保証システムであって、データ真正性保証サーバは、所定のタイミングで、業務処理システム内の真正性保証対象のファイルを大容量記憶装置にバックアップする手段と、手段によるバックアップに伴い、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ハッシュ値をメモリに保存する手段と、ファイルについての真正性検証の要求に基づき、ファイルを業務処理システムから読み込み、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ファイルについての前回のハッシュ時のハッシュ値をメモリから読み出し、新たに生成したハッシュ値と比較してデータ真正性の検証を行う手段と、ハッシュ値比較の結果、不一致の場合、ファイルについてデータ改ざんが発生したと判断し、ファイルを大容量記憶装置に保存されているバックアップファイルをもとに復元する手段とを有することを特徴としている。

【0008】請求項2記載の発明は、請求項1記載の発明において、バックアップに伴うハッシュの際、ハッシュ値に電子署名を付加する手段と、データ真正性検証の際、前回のハッシュ値に付加されている電子署名の正当性を検証する手段とをさらに有することを特徴としている。

【0009】請求項3記載の発明は、請求項記載の発明において、ファイルについての真正性検証の過程を履歴ファイルに記録する手段をさらに有することを特徴としている。

【0010】請求項4記載の発明は、請求項1または2に記載の発明において、ファイルについての真正性検証の結果を管理者に通知する手段をさらに有することを特徴としている。

【0011】請求項5記載の発明は、業務処理システムの保持するファイルについてデータの真正性を保証する簡易型データ真正性保証方法であって、データ真正性保証サーバが、所定のタイミングで、業務処理システム内の真正性保証対象であるファイルを大容量記憶装置にバックアップするステップと、バックアップに伴い、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ハッシュ値をメモリに保存するステップと、ファイルについての真正性検証の要求に基づき、ファイルを業務処理システムから読み込み、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ファイルについての前回のハッシュ時のハッシュ値をメモリから読み出し、新たに生成したハッシュ値と比較してデータ真正性の検証を行うステップと、ハッシュ値比較の結果、不一致の場合、ファイルについてデータ改ざんが発生したと判断し、ファイルを大容量記憶装置に保存されているバックアップファイルをもとに復元するステップとを有す

ることを特徴としている。

【0012】請求項6記載の発明は、請求項5記載の発明において、バックアップに伴うハッシュの際、ハッシュ値に電子署名を付加するステップと、データ真正性検証の際、前回のハッシュ値に付加されている電子署名の正当性を検証するステップとをさらに有することを特徴としている。

【0013】請求項7記載の発明は、請求項5または6に記載の発明において、ファイルについての真正性検証の過程を履歴ファイルに記録するステップをさらに有することを特徴としている。

【0014】請求項8記載の発明は、請求項5から7のいずれか1項に記載の発明において、ファイルについての真正性検証の結果を管理者に通知するステップをさらに有することを特徴としている。

【0015】請求項9記載の発明は、業務処理システムの保持するファイルについてデータの真正性を保証する簡易型データ真正性保証プログラムであって、データ真正性保証サーバに、所定のタイミングで、業務処理システム内の真正性保証対象であるファイルを大容量記憶装置にバックアップする処理と、バックアップに伴い、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ハッシュ値をメモリに保存する処理と、ファイルについての真正性検証の要求に基づき、ファイルを業務処理システムから読み込み、ファイルを引数としてハッシュ関数によりハッシュ値を生成し、ファイルについての前回のハッシュ時のハッシュ値をメモリから読み出し、新たに生成したハッシュ値と比較してデータ真正性の検証を行う処理と、ハッシュ値比較の結果、不一致の場合、ファイルについてデータ改ざんが発生したと判断し、ファイルを大容量記憶装置に保存されているバックアップファイルをもとに復元する処理とを実行させることを特徴としている。

【0016】請求項10記載の発明は、請求項9記載の発明において、データ真正性保証サーバに、バックアップに伴うハッシュの際、ハッシュ値に電子署名を付加する処理と、データ真正性検証の際、前回のハッシュ値に付加されている電子署名の正当性を検証する処理とをさらに実行させることを特徴としている。

【0017】請求項11記載の発明は、請求項9または10に記載の発明において、データ真正性保証サーバに、ファイルについての真正性検証の過程を履歴ファイルに記録する処理をさらに実行させることを特徴としている。

【0018】請求項12記載の発明は、請求項9から11のいずれか1項に記載の発明において、データ真正性保証サーバに、ファイルについての真正性検証の結果を管理者に通知する処理をさらに実行させることを特徴としている。

【0019】

【発明の実施の形態】以下、本発明の実施の形態を添付図面を参照しながら詳細に説明する。

【0020】図1は、本発明の第1の実施の形態における簡易型データ真正性保証システムの構成を示す図である。このシステムは、企業や行政機関などのイントラネット（インターネット技術を利用した内部ネットワーク）などにおいて実現されるものであり、一般業務処理システム100と、文書保存装置200と、データ真正性保証サーバ300とを構成要素として有する。

【0021】一般業務処理システム100は、業務処理のためのデータファイルを扱っており、このデータファイルを保存するデータベースを有する。本システムは、このデータファイルについての真正性の保証を行うものである。以下、この真正性保証の対象であるデータファイルを、単に「対象ファイル」と呼ぶ。

【0022】文書保存装置200は、大容量バックアップファイル格納部201を有する。これは、例えば、磁気ディスクや磁気テープなどの安価な記憶装置である。対象ファイルは、データ真正性保証サーバ300により、この大容量バックアップファイル格納部201にバックアップされる。

【0023】データ真正性保証サーバ300は、データバックアップ処理部301と、ハッシュ値作成処理部302と、データ真正性検証処理部303と、データ復元処理部304とを有する。データ真正性保証サーバ300は、本発明の簡易型データ真正性保証プログラムに従って動作する。

【0024】データバックアップ処理部301は、対象ファイルについて、所定のタイミングで文書保存装置200へバックアップする処理を行う。対象ファイルのバックアップは、ファイル新規作成時、更新時、あるいは、所定の一括バックアップ時などに行われるように予め設定される。

【0025】ハッシュ値作成処理部302は、対象ファイルについて、ハッシュ関数によりハッシュ値を作成し、サーバ300内の記憶スペース（データベース）に保存する処理を行う。ハッシュ値の作成は、上記バックアップ処理に伴って行われる。このハッシュ関数は、2つの異なる入力データから同一のハッシュ値を返す確率がほぼゼロであるという性質を持つ。また、可変長データを入力して、固定長データを出力する性質を持つ。また、ハッシュ値から入力データを推測することが困難であるという性質を持つ。

【0026】データ真正性保証サーバ300内に保存するハッシュ情報の例を図5に示す。図5において、「FileID」と「Hash値」は必須要素である。「FileID」は、対象ファイルを一意に識別する。「属性」は対象ファイルについての種々の属性を示す。「Hash日時」は、そのファイルについて最後にハッシュを行った日時である。「Hash値」は、そのファイル

についてのハッシュ値を示す。

【0027】データ真正性検証処理部303は、対象ファイルについてのデータ真正性検証の要求に基づき、一般業務処理システム100から対象ファイルを読み込み、この対象ファイルについて上記ハッシュ関数によりハッシュ値を演算する（※この対象ファイルについての前回のハッシュ時と同じアルゴリズムのハッシュ関数を用いる必要がある）。そして、この対象ファイルについての前回のハッシュ値をサーバ300内から読み出し、今回のハッシュ値と比較して真正性の検証を行う。前述したように、ハッシュ関数は、入力するデータが同一の場合に同一のハッシュ値を返す性質を持つ。よって、上記二回のハッシュ処理の間に対象ファイルに改変（侵入者による改ざんなど）が加えられている場合、ハッシュ関数は異なる値を返すことになるため、データの改ざんを検出することができる。データ真正性検証部303は、ハッシュ値が不一致の場合、対象ファイルについて改ざんが発生したと判断する。

【0028】対象ファイルについて真正性検証を行うタイミングとしては、以下のようなものが考えられる。

1) 一般業務処理システム100における対象ファイルへのアクセス時に自動的に行う（一般業務処理システム100がデータ真正性保証サーバ300に対し検証要求を発行する）。2) 予め設定された周期や時刻で自動的に行う。3) 文書管理責任者の意志により任意タイミングで行う。

【0029】データ復元処理部304は、対象ファイルについてのデータ真正性検証の結果、改ざんが発生したと判断された場合に、文書保存装置200に保存されているバックアップファイルをもとに自動的に対象ファイルの復元を行う。

【0030】図3は、第1の実施の形態における簡易型データ真正性保証システムの動作を示すフローチャートである。以下、図3に沿って説明する。まず、ある対象ファイル（=iとする）について、バックアップイベントが発生する（バックアップのタイミングについては前述）（ステップS1）。一般業務処理システム100は、データ真正性保証サーバ300に対し、バックアップ処理の要求を行う（ステップS2）。データ真正性保証サーバ300のデータバックアップ処理部301は、一般業務処理システム100の要求に基づき、バックアップ対象である対象ファイルiについて、文書保存装置200の大容量バックアップファイル格納部201にバックアップする（ステップS3）。

【0031】対象ファイルiについてのこのバックアップ処理に伴って、データ真正性保証サーバ300は、ハッシュ値作成処理部302により、対象ファイルiを読み込み、この対象ファイルiを入力データとしてハッシュ関数によりハッシュ値hiを演算して（ステップS4）、データ真正性保証サーバ300内の所定の記憶ス

ベース（データベース）に格納する（ステップS5）。

【0032】所定のタイミングで、対象ファイルiについて、データ真正性検証イベントが発生する（ステップS6）。一般業務処理システム100は、データ真正性保証サーバ300に対し、対象ファイルiについての、真正性検証の要求を行う（ステップS7）。データ真正性保証サーバ300は、一般業務処理システム100からの要求に回答する。データ真正性保証サーバ300のデータ真正性検証処理部303は、要求に応じて、一般業務処理システム100から対象ファイルiを読み取り（ステップS8）、前述のバックアップ時のハッシュと同一のハッシュ関数によりハッシュ値hi'を演算する（ステップS9）。データ真正性検証処理部303は、この対象ファイルiについての前回のハッシュ時のハッシュ値hiをサーバ300内から読み出す（ステップS10）。そして、ハッシュ値hiとhi'とを比較して真正性の検証を行う（ステップS11）。

【0033】比較の結果、ハッシュ値が一致する場合、データ真正性保証サーバ300は、前回のハッシュ時と今回のハッシュ時の間に、対象ファイルiのデータ改ざんは発生していないと判断する。ハッシュ値が不一致の場合、データ真正性保証サーバ300は、前回のハッシュ時と今回のハッシュ時の間に、対象ファイルiのデータ改ざんが発生したと判断する。そして、自動的に、文書保存装置200の大容量バックアップファイル格納部201に格納されているバックアップファイルをもとに、一般業務処理システム100内の改ざんが発生したと考えられる対象ファイルiを置き換えてデータの復元（リストア）を行う（ステップS12）。

【0034】なお、その他の処理として、データ真正性保証サーバ300が、以上のようなデータ検証の過程を履歴ファイルに記録することにより、文書管理責任者は、後刻、対象ファイルについて改ざんが発生しているかどうかを認識できる。また、対象ファイルの性質によっては、データ改ざん発生時に、文書管理責任者にその旨を通知するような構成にすることが考えられる（検証後処理：ステップS13）。

【0035】図2は、本発明の第2の実施の形態における簡易型データ真正性保証システムの構成を示す図である。第2の実施例は、第1の実施例の機能に加え、さらにハッシュ値に対する電子署名機能を備える。図2を参照すると、第2の実施例におけるデータ真正性保証システムは、一般業務処理システム400と、文書保存装置500と、データ真正性保証サーバ600と、を有する。

【0036】一般業務処理システム400および文書保存装置500の構成および機能は、第1の実施例における一般業務処理システム100および文書保存装置200と同様である。

【0037】データ真正性保証サーバ600は、データ

バックアップ処理部601、ハッシュ値作成処理部602、電子署名処理部603、データ真正性検証処理部604、および、データ復元処理部605を有する。電子署名処理部603以外の各部は、第1の実施例におけるデータ真正性保証サーバ300の構成および機能と同様である。

【0038】電子署名処理部603は、ハッシュ値作成処理部602によって生成された対象ファイルについてのハッシュ値に対し、さらに電子署名を付加する処理を行う。また、真正性検証時に、署名の正当性を検証する処理を行う。これにより、データ真正性保証サーバ600に保存されているハッシュ値についての信頼性を高める。

【0039】第2の実施例での全体の処理の流れを図5に示す。特に、電子署名付加処理の例について図6および図7を参照して説明する。処理の流れは以下のようになる。まず、対象ファイルのバックアップに伴うハッシュ時には、1)ハッシュ値作成処理部602は、対象ファイル*i*について、ハッシュ関数Hash1()を用いてハッシュ値*h_i*を生成する。2)電子署名処理部603は、ハッシュ値*h_i*をさらに所定の電子署名用ハッシュ関数Hash2()によりハッシュして*h_d*(ダイジェスト)を生成する。2)電子署名処理部603は、*h_d*を文書管理責任者の秘密鍵(署名生成鍵)により暗号化して署名データ*s*を作成する。3)電子署名処理部603は、署名データ*s*をもとのハッシュ値*h_i*に付加して一緒に保存する。

【0040】データ真正性検証時には、上記のプロセスを逆に辿ることになる。即ち、データ真正性検証処理部604は、1)対象ファイル*i*について、ハッシュ関数Hash1()によりハッシュを行いハッシュ値*h_i'*を生成する。2)対象ファイル*i*についての前回のハッシュ情報(ハッシュ値*h_i*+署名データ*s*)を読み出し、署名データ*s*を文書管理責任者の公開鍵(署名検証鍵)により復号化し、*h_d'*を得る。署名が正当なものであれば、これは*h_d*と等しい。3)対象ファイル*i*についての前回のハッシュ値*h_i*を署名用ハッシュ関数Hash2()によりハッシュし、*h_d*を得る。4)上記値*h_d*と*h_d'*とを比較して署名の正当性を検証する。署名の正当性が確認されると、添付のハッシュ値*h_i*の正当性が保証される。5)上記*h_i'*と*h_i*とを比較し、対象ファイル*i*についての真正性検証を行う。

【0041】なお、文書管理責任者が交代するたびに、署名が付加されたハッシュ値の上にさらに異なる署名を付加する構成にすることにより、データ真正性保証の強化を図ることもできる。

【0042】なお、上述した実施形態は、本発明の好適な実施形態の一例を示すものであり、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲内において、種々変形実施が可能である。

【0043】

【発明の効果】以上の説明から明らかなように、本発明によれば、イントラネットなどにおいて特別なハードウェア装置を必要とせずに安価な構成で業務処理ファイルなどのデータの真正性を保証するシステム、方法、およびプログラムを提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における簡易型データ真正性保証システムの構成を示す図である。

【図2】本発明の第2の実施の形態における簡易型データ真正性保証システムの構成を示す図である。

【図3】本発明の第1の実施の形態における簡易型データ真正性保証システムの動作を示すシーケンス図である。

【図4】本発明の第2の実施の形態における簡易型データ真正性保証システムの動作を示すシーケンス図である。

【図5】データ真正性保証サーバ300に保存されるハッシュ情報を示す図である。

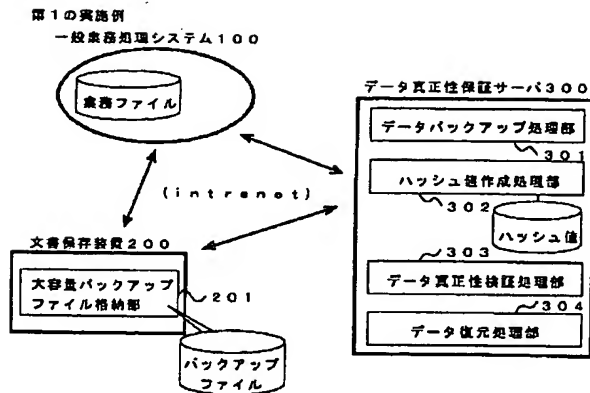
【図6】ハッシュ値に対する電子署名付加処理(バックアップに伴うハッシュ時)について示す図である。

【図7】ハッシュ値に対する電子署名付加処理(真正性検証時)について示す図である。

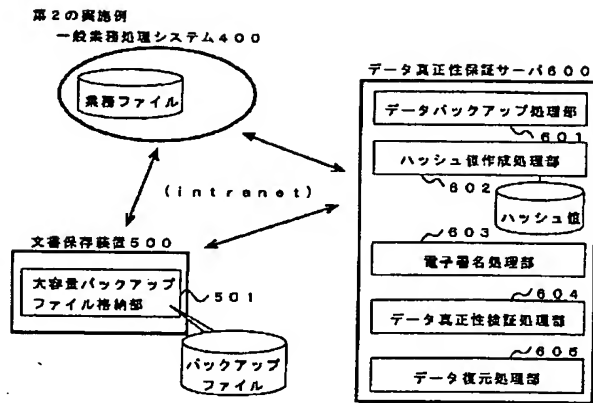
【符号の説明】

- 100 一般業務処理システム
- 200 文書保存装置
- 201 大容量バックアップファイル格納部
- 300 データ真正性保証サーバ
- 301 データバックアップ処理部
- 302 ハッシュ値作成処理部
- 303 データ真正性検証処理部
- 304 データ復元処理部
- 400 一般業務処理システム
- 500 文書保存装置
- 501 大容量バックアップファイル格納部
- 600 データ真正性保証サーバ
- 601 データバックアップ処理部
- 602 ハッシュ値作成処理部
- 603 電子署名処理部
- 604 データ真正性検証処理部
- 605 データ復元処理部

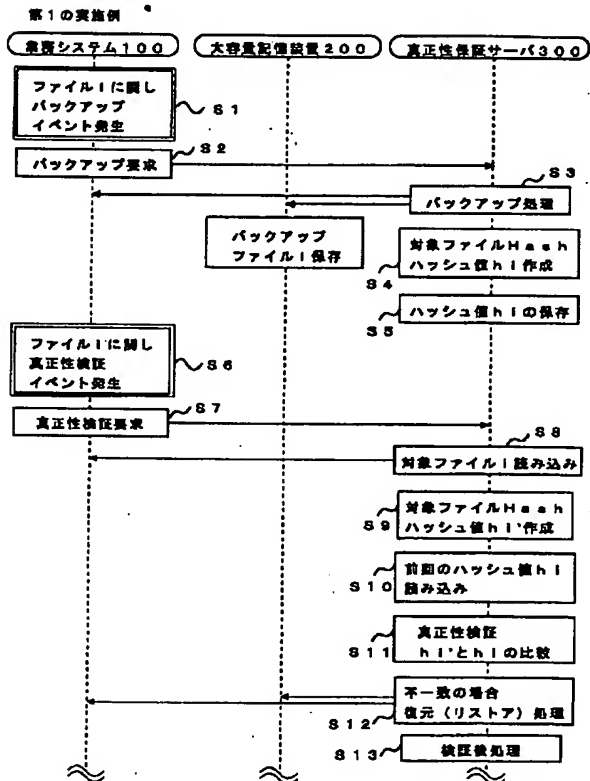
【図1】



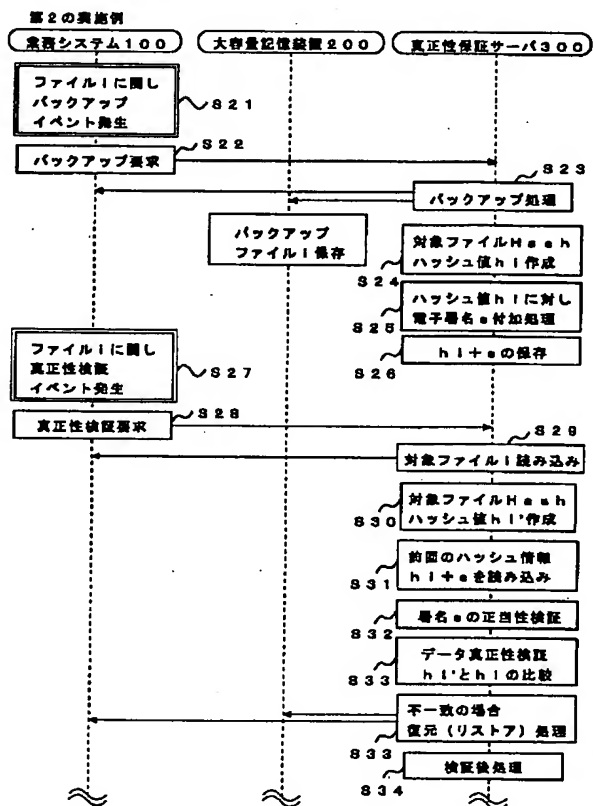
【図2】



【図3】



【図4】

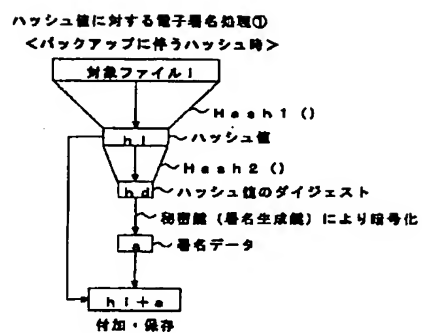


【図5】

データ真正性保証サーバに保存するハッシュ情報

FileID	属性	Hash日時	Hash値	...

【図6】



【図7】

